Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] What is claimed is:

1.A system for actively updating a cryptography module in a security gateway, the security gateway connected between a user computer system and a network system, the system comprising:

a Web GUI for generating at least one window in the user computer system, the window having a decryption/encryption module update system to allow a user to upload a new decryption/encryption module to the security gateway by the Web GUI;

an extended library for accommodating a decryption/encryption module; and

a module update unit for actively updating a corresponding decryption/encryption module in the extended library according to the new decryption/encryption module uploaded to the security gateway or adding the uploaded decryption/encryption module into the extended library.

[c2] 2.The system of claim 1 wherein the security gateway is a VPN gateway complying with an IPSEC protocol.

[c3] 3.The system of claim 1 wherein the security gateway in-

cludes a current library, a kernel, and a daemon, the module update unit being located in the current library.

[c4] 4.The system of claim 1 wherein the decryption/encryption module update system in the window of the Web GUI includes a system for allowing the user to update a current decryption/encryption module in the security gateway.

[c5] 5.The system of claim 4 wherein the decryption/encryption module update system in the window of the Web GUI further includes a defined decryption/encryption module system for allowing the user to add a defined decryption/encryption module into the security gateway.

[c6] 6.The system of claim 5 further comprising a defined module unit connected to the defined decryption/encryption module system for generating a window for providing the user with an instruction to fill in a field in the window with a description of the defined decryption/encryption module.

[c7] 7.The system of claim 6 wherein the description of the defined decryption/encryption module includes an algorithm, algorithmic identifier, data encryption block size, key length, and decryption/encryption executing function, the parameters of the decryption/encryption exe-

cuting function including a data address, data block size, key information, key length, initial vector, and decryption/encryption flag.

[c8] 8.The system of claim 1 wherein the module update unit selects to actively update the corresponding decryption/encryption module in the extended library or to add the uploaded decryption/encryption module into the extended library according to the new decryption/encryption module.

[c9] 9.The system of claim 2 further comprising an extended library interface for assisting the extended library to communicate with the current library and the kernel.

[c10] 10.The system of claim 1 further comprising a configuration set unit such as a system file for setting an execution process according to an IPSEC protocol wherein after a decryption/encryption module is updated or added, the key exchange process is updated according to an IKE protocol.

[c11] 11. A method for actively updating a cryptography module in a security gateway, the security gateway connected between a user computer system and a network system, the method comprising:
downloading a new decryption/encryption module to the

user computer system through the network system;
starting a Web GUI of the security gateway for generating at least one window in the user computer system, the window having a decryption/encryption module update system;
selecting a decryption/encryption module from the window provided by the Web GUI;
uploading the selected decryption/encryption module to the security gateway;
a module update unit of the security gateway actively updating a corresponding decryption/encryption module in the extended library according to the uploaded decryption/encryption module or adding the uploaded decryption/encryption module into the extended library; and
updating a key exchange process in the security gateway according to an IKE protocol.

[c12] 12.The method of claim 11 wherein the decryption/encryption module update system in the window of the Web GUI includes a system for allowing the user to update a current decryption/encryption module in the security gateway.

[c13] 13.The method of claim 12 wherein the decryption/encryption module update system in the window of the Web GUI further includes a defined decryption/encryp-

tion module system for allowing the user to add a defined decryption/encryption module into the security gateway.

[c14] 14.The method of claim 13 further comprising:
when starting the defined decryption/encryption module, generating a window for providing a user with an instruction to fill in a field in the window with a description of the defined decryption/encryption module.

[c15] 15.The method of claim 14 wherein the descriptions of the defined decryption/encryption module includes an algorithm, algorithmic identifier, data encryption block size, key length, and decryption/encryption executing function, the parameters of the decryption/encryption executing function including a data address, data block size, key information, key length, initial vector, and decryption/encryption flag.

[c16] 16.The method of claim 11 further comprising:
the security gateway executing the updated key exchange process.

[c17] 17.A key exchange process in a security gateway according to an IKE protocol, the key exchange process comprising:
(a) initiating a current IPSEC security association (SA) of

the security gateway;

(b) executing an IKE phase 1;

(c) if there is no appropriate decryption/encryption module in a current library of the security gateway, selecting an appropriate decryption/encryption module from an extended library of the security gateway;

(d) executing an IKE phase 2;

(e) repeating step (c);

(f) completing the key exchange process of the IKE phase 1 and 2; and

(g) informing the kernel of the security gateway of an update to the current IPSEC SA.